U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

January 29, 2024

BY ECF and Email
The Honorable Paul A. Crotty
United States District Judge
Southern District of New York
500 Pearl Street
New York, NY 10007

Re: *United States v. Daniel Abayev and Peter Leyman*, 22 Cr. 655 (PAC)

Dear Judge Crotty:

The Government respectfully submits this letter in advance of the February 12, 2024, sentencing of defendants Daniel Abayev and Peter Leyman after their guilty pleas. The defendants engaged in a years-long scheme to hack the electronic taxi dispatch system at John F. Kennedy International Airport. The stipulated Guidelines range for Abayev is 60 months, which is the statutory maximum. The stipulated Guidelines range for Leyman is 57 to 60 months. For both defendants, a sentence at or within the stipulated Guidelines range would not be greater than necessary to serve the purposes of sentencing.

I. The Offense Conduct

A. The Taxi Dispatch Hacking Scheme

From approximately 2019 until 2021, Abayev, Leyman, and others engaged in a scheme (the "Hacking Scheme") to hack the electronic taxi dispatch system (the "Dispatch System") at John F. Kennedy International Airport ("JFK").

Taxi drivers who sought to pick up a fare at JFK were required to wait in a holding lot at JFK before being dispatched to a specific terminal by the Dispatch System. Taxi drivers often waited several hours in the lot before being dispatched to a terminal, and were dispatched in approximately the order in which they arrived at the holding lot.

Beginning in approximately November 2019, Abayev, Leyman, and two Russian hackers named Aleksandr Derebentc and Kirill Shipulin began exploring various means to access the Dispatch System, including bribing someone to insert a flash drive containing malware into computers connected to the Dispatch System, obtaining unauthorized access to the Dispatch System via a Wi-Fi connection, and stealing computer tablets connected to the Dispatch System.

The Hacking Scheme successfully gained access to the Dispatch System and the ability to manipulate it in approximately November 2019. The hackers used their unauthorized access to the Dispatch System to alter the Dispatch System and move specific taxis to the front of the line, thereby allowing the drivers of those specific taxis to skip other taxi drivers who had arrived at the holding lot earlier and avoid time waiting in the holding lot.

Members of the Hacking Scheme charged individual taxi drivers $10 each time they were advanced to the front of the line. Individual taxi drivers paid the members of the Hacking Scheme in a variety of ways, including through a mobile payment system or in cash. Taxi drivers learned that they could skip the taxi line by paying $10 to members of the Hacking Scheme through word of mouth, and members of the Hacking Scheme offered some taxi drivers waivers of the $10 fee in exchange for recruiting other taxi drivers to pay the $10 fee to skip the taxi line. In some cases, brokers purchased trips in bulk from the members of the Hacking Scheme, and then gave those trips to taxis they controlled.

Members of the Hacking Scheme used large group chat threads to manage the scheme and communicate with the dozens or hundreds of taxi drivers who took advantage of the scheme. For example, when the Hacking Scheme had access to the Dispatch System for the day, a member of the Hacking Scheme would message the group chat threads, "Shop open." When the Hacking Scheme's access to the Dispatch System was interrupted, a member of the Hacking Scheme would message the group chat threads, "Shop closed." Members of the Hacking Scheme also directed taxi drivers how to avoid being detected by law enforcement. In order to skip the taxi line, taxi drivers would message their taxi medallion numbers into the group chat threads, and a member of the Hacking Scheme would then send a message to the taxi driver with the terminal that the driver should go to in order to skip the taxi line and pick up a fare.

During the periods of time when the Hacking Scheme had successful access to the Dispatch System, it was highly lucrative. The scheme sold hundreds of trips per day, and sometimes as many as a thousand trips in a day.

Abayev and Leyman engaged in the scheme from New York, and Derebentc and Shipulin generally did so from Russia. The four shared the profits from the scheme. In order to transfer a portion of the cash they collected back to Derebentc and Shipulin, Abayev and Leyman sent the money by wire or using other means. Abayev and Leyman sometimes falsely described these transfers of the profits of the Hacking Scheme to their banks as "payment for software development" or "payment for services rendered."

From approximately 2019 until 2021, employees of JFK repeatedly attempted to secure the Dispatch System from the members of the Hacking Scheme and to eject them from the system. Those efforts were periodically successful, but the members of the Hacking Scheme repeatedly devised new methods to access the Dispatch System and regain their control of the Dispatch System so the scheme could continue. Some of those new methods involved corrupting employees at JFK to assist them in providing access. The otherwise highly lucrative Hacking Scheme was periodically disrupted in this way, and was also disrupted by the dramatic decrease in air traffic caused by the COVID-19 pandemic that began in approximately March 2020.

B. The Respective Roles of Abayev and Leyman

Abayev was one of the leaders of the Hacking Scheme. He conceived of the scheme and, while he was abroad, recruited Derebentc to handle the technical aspects of the scheme.

While Abayev was in the United States, he communicated frequently with Derebentc and Shipulin about the attempts to hack the Dispatch System. Derebentc and Shipulin kept Abayev apprised of the status of their hacking efforts, and Abayev followed technical instructions provided by Derebentc and Shipulin to assist in the hacking. For example, early in the scheme, Abayev messaged Derebentc, "I know that the Pentagon is being hacked. So, can't we hack the taxi industry." Due to concerns about detection by law enforcement, Abayev began using the encrypted messaging application Telegram to communicate during the scheme.

Abayev also led the communications with taxi drivers, including the sale of trips to taxi drivers and the collection of money from them. He also directed the taxi drivers how to best evade detection by law enforcement. For example, in one of the large group chats with taxi drivers, Abayev sent the following message to ensure that law enforcement would not detect the Hacking Scheme:

> DEAR DRIVERS !!!! PLEASE !!!!
> Do not wait at the gas station in JFK
> Please do not go around the CTH Lot 👨✈
> Please do not wait at Rockway av 👮
> You have to be very very carefully 👮👮

He also tracked the profits of the scheme and controlled the redistribution of the profits among the coconspirators. For example, Abayev messaged Leyman the following spreadsheet that listed the exact numbers of sales of trips each day, based on the broker who bought the trips.

DAY		TOTALS FOR A DAY	5L46 RICHARD	8Y78 ISAAC	AFRIFA	ALEX	BACK	BORIS	CALY	DENNIS	JAY	JOE	LEONID	LUCY	MAN	OPM	RD	RICKY	SHAVKAT
MONDAY	ALL	295	1	1	1	37	64	11	2	1	16	1	4	1	34	21	14	21	37
MONDAY	KICKED	14	0	0	0	4	3	0	0	0	2	0	0	0	1	0	0	1	2
MONDAY	FREE	25	0	0	0	4	0	2	0	0	0	0	4	0	5	2	0	2	5
MONDAY	CANCELED	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
MONDAY	CLEAN	256	1	1	1	29	61	9	2	1	14	1	0	1	28	19	14	18	30
MONDAY	NOTES					RAZNICA 1 RABOTA	HAS 60 3 MORE KICKED?												

DAY		TOTALS FOR A DAY	5L46 RICHARD	8Y78 ISAAC	9N54 GIDEON	AFRIFA	ALEX	BACK	BORIS	CALY	DENNIS	JAY	LEONID	LUCY	MAN	NANA	OPM	RD	RICKY
TUESDAY	ALL	352		2	1	1	34	67	15	1	1	12	3	2	39	2	38	16	15
TUESDAY	KICKED	7		0	0	0	0	3	0	0	0	0	0	0	3	0	0	0	0
TUESDAY	FREE	20		0	0	0	0	2	0	0	0	0	3	0	0	0	6	0	0
TUESDAY	CANCELED	0			0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TUESDAY	CLEAN	325	0	2	1	1	34	64	13	1	1	12	0	2	36	2	32	16	15

DAY		TOTALS FOR A DAY	5L46 RICHARD	8Y78 ISAAC	ALEX	BACK	BORIS	CALY	DENNIS	JAY	JOE	LEONID	LUCY	MAN	MARTIN	OPM	RD	8K38 RICKY	SHAVKAT
WEDNESDAY	ALL	420	1	1	42	80	15	2		30	1	5	4	53	1	46	21	16	34
WEDNESDAY	KICKED	9	0	0	0	0	0	0		2	0	0	0	1	0	3	0	0	3
WEDNESDAY	FREE	31	0	0	4	0	3	0		0	0	5	0	5	0	3	0	0	6
WEDNESDAY	CANCELED	1	0	0	0	0	0	0		0	0	0	0	1	0	0	0	0	0
WEDNESDAY	CLEAN	379	1	1	38	80	12	2	0	28	1	0	4	46	1	40	21	16	25

On another day, Abayev bragged about the success of the scheme: "On our end this is absolutely a record. Here we almost have 600. We netted at least 500. This has never happened before. . . . This is exactly the level that I want to have every day. . . Now in the morning we are going to collect the dough."

Similarly, Abayev arranged the redistribution of profits among the coconspirators. He and Leyman each kept 25% of the total profits of the Hacking Scheme, and sent 50% of the profits to Derebentc and Shipulin. Abayev coordinated and directed the international payments back to Derebentc and Shipulin.

Abayev had limited technical expertise. While he conceived of the scheme and directed it, he would not have been able to actually hack the Dispatch System without the expertise of Derebentc and Shipulin.

Leyman's role was substantially less than Abayev's. Leyman's primary job was to collect the payments from individual taxi drivers and brokers, which primarily took the form of cash. Leyman appears to have had little or no direct contact with Derebentc or Shipulin.

II. Procedural History

On December 5, 2022, a grand jury indicted Abayev and Leyman on two counts each of conspiracy to commit computer intrusion for their role in the taxi hacking scheme. Law enforcement arrested Abayev and Leyman on the indictment on December 20, 2022.

On October 5, 2023, Leyman pleaded guilty to one count of conspiracy to commit computer intrusion, in violation of 18 U.S.C. § 371. On October 30, 2023, Abayev also pleaded guilty to one count of conspiracy to commit computer intrusion, in violation of 18 U.S.C. § 371.

Two other defendants, Aleksandr Derebentc and Kirill Shipulin, have also been charged in unsealed indictments for their role in the scheme. Both those defendants reside in Russia and remain fugitives.

III. The Sentencing Guidelines Ranges

Both defendants entered into plea agreements when they pleaded guilty, and those plea agreements contain stipulated Guidelines ranges.

A. Abayev

As to Abayev, the base offense level for the computer intrusion conspiracy is six: 16 levels are added because the loss amount is more than $1,500,000 but less than $3,500,000; two levels are added because a substantial part of the fraudulent scheme was committed from outside the United States—from Russia—or because the offense otherwise involved sophisticated means and the defendant intentionally engaged in or caused the conduct constituting sophisticated means; four levels are added because the defendant was convicted of an offense under 18 U.S.C.

§ 1030(a)(5)(A); four levels are added because the defendant was an organizer or leader of a criminal activity that involved five or more participants or was otherwise extensive; and three levels are subtracted because the defendant accepted responsibility for his crime.

While Abayev does not dispute that any of the enhancements apply—and in fact he explicitly agreed to each in his plea agreement—he suggests that they overstate his culpability and reflect issues with the Guidelines themselves. In each case, he is wrong:

- **Loss.** The defendant complains that the loss number in this case overstates his culpability. Abayev Memo at 1-2. That is not correct for several reasons. *First*, it is common for the loss in hacking crimes to be far higher than the gain to the defendants. Hacking frequently imposes huge responsive costs on victims, and the gains by perpetrators can be fairly small in comparison. In recognition of that fact, the Guidelines specifically provide for a broad definition of loss when it comes to computer fraud.[1] *Second*, the loss amount in this case was the subject of extensive negotiation and discussion with both defendants. The victim in this case—the Port Authority—initially identified its total loss as over $7 million. After hearing the defendants' arguments that they should not be held fully responsible for the cost of the upgrade to the Dispatch System, the Government agreed to reduce the loss to3,456,169.50, and both defendants agreed that number was the correct loss amount. In other words, the loss amount in this case has already been adjusted significantly downward to account for the exact arguments Abayev repeats in his sentencing memo. *Third*, the defendants are properly held responsible for the costs of the upgrade. The Hacking Scheme went on for years, and the conspirators repeatedly developed new methods to access the Dispatch System as soon as a prior vulnerability was fixed. JFK was forced to upgrade because all its other attempts to defeat the Hacking Scheme had failed.

- **Scheme Committed from Outside the United States or Sophisticated Means.** Section 2B1.1(b)(10) provides for a two-level enhancement if *either* of the following conditions are met: "(B) a substantial part of a fraudulent scheme was committed from outside the United States; or (C) the offense otherwise involved sophisticated means and the defendant intentionally engaged in or caused the conduct constituting sophisticated means." Here, *both* are met. First, a large part of the scheme was carried out from Russia. The Guidelines properly provide an enhancement in such cases, both because it demonstrates the sophistication of the scheme and because the international component makes detection and prosecution of the crime substantially more difficult. Second, while Abayev may not have personally done the hacking—which was undoubtedly sophisticated—he recruited the hacker and directed the hack, and therefore plainly personally "caused the conduct constituting sophisticated means."

[1] *See* U.S.S.G. 2B1.1 n. 3(A)(v)(III) ("In the case of an offense under 18 U.S.C. § 1030, actual loss includes the following pecuniary harm, regardless of whether such pecuniary harm was reasonably foreseeable: any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service.")

- **Section (a)(5)(A) Conviction.** Section 2B1.1(b)(1)(ii) provides for a four-point enhancement if the defendant was convicted of a violation of 18 U.S.C. § 1030(a)(5)(A), as both defendants were. Abayev's submission suggests that this enhancement applies "simply because the offense was committed with a computer." Abayev Memo at 4. Not so. Section 1030(a), the statute criminalizing computer intrusion, sets forth seven different crimes, each with various sub-crimes. Only one of those, for a defendant who, "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer," is subject to the four-point enhancement. That is precisely what the members of the Hacking Scheme did. Every day when the scheme successfully operated, they deleted the correct data about each taxi's place in line and replaced it with their own corrupted data. The Guidelines properly provide an enhancement for deliberate damage of that kind, as opposed to simple unauthorized access.

- **Leadership.** Abayev complains that a four-point leadership enhancement overstates his culpability. Abayev Memo at 3. Abayev conceived of the scheme, recruited the participants, directed the scheme, and controlled the division of the profits. He is plainly an organizer or leader, and in fact agreed in his plea agreement that he is one. Leaders of criminal conduct properly face more serious punishment than other participants.

Abayev also argues that he is also eligible for a two-level reduction pursuant to Section 4C1.1. Abayev Memo at 5. However, the defendant received an aggravated role enhancement under Section 3B1.1 of the Guidelines, and is therefore barred from receiving the Section 4C1.1 reduction. *See* U.S.S.G. § 4C1.1(a)(10).

The total offense level is accordingly 29, and the defendant has no prior convictions, so his criminal history category is I. The resulting Guidelines range is 87 to 108 months. However, the statutory maximum term of imprisonment is 60 months, and so 60 months becomes the Guidelines range.

Probation recommends a sentence of 60 months, and Abayev requests a non-incarceratory sentence.

B. Leyman

The offense level calculation for Leyman is identical to Abayev's except that Leyman does not receive any leadership points. The base offense level for the computer intrusion conspiracy is six; 16 levels are added because the loss amount is more than $1,500,000 but less than $3,500,000; two levels are added because a substantial part of the fraudulent scheme was committed from outside the United States or because the offense otherwise involved sophisticated means and the defendant intentionally engaged in or caused the conduct constituting sophisticated means; four levels are added because the defendant was convicted of an offense under 18 U.S.C. § 1030(a)(5)(A); and three levels are subtracted because the defendant accepted responsibility for his crime.[2]

[2] Leyman does not receive a reduction pursuant to Section 4C1.1 because of his prior conviction.

The total offense level is accordingly 25. Leyman has a 2015 conviction for criminal possession of stolen property, for which he receives one criminal point, and his criminal history category is therefore I. The resulting Guidelines range is 57 to 71 months, but because the statutory maximum is 60 months, the resulting Guidelines range is 57 to 60 months.

Probation recommends a sentence of 36 months, and Leyman requests a non-incarceratory sentence.

IV. The Appropriate Sentence

A. Applicable Law

While advisory following *United States v. Booker*, 543 U.S. 220 (2005), the Guidelines remain "the starting point and the initial benchmark" for sentencing. *Gall v. United States*, 552 U.S. 38, 49 (2007). That is because the Guidelines are "the product of careful study based on extensive empirical evidence derived from the review of thousands of individual sentencing decisions." *Id.* at 46. For that reason, "in the overwhelming majority of cases, a Guidelines sentence will fall comfortably within the broad range of sentences that would be reasonable in the particular circumstances." *United States v. Fernandez*, 443 F.3d 19, 27 (2d Cir. 2006).

In imposing a sentence, the Court must consider seven factors outlined in Title 18, United States Code, Section 3553(a): (1) "the nature and circumstances of the offense and the history and characteristics of the defendant"; (2) the four legitimate purposes of sentencing, as set forth below; (3) "the kinds of sentences available"; (4) the Guidelines range itself; (5) any relevant policy statement by the Sentencing Commission; (6) "the need to avoid unwarranted sentence disparities among defendants"; and (7) "the need to provide restitution to any victims," 18 U.S.C. § 3553(a)(l)–(7). *See Gall,* 552 U.S. at 50 & n.6.

In determining the appropriate sentence, the statute directs judges to "impose a sentence sufficient, but not greater than necessary, to comply with the purposes" of sentencing, which are:

(A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
(B) to afford adequate deterrence to criminal conduct;
(C) to protect the public from further crimes of the defendant;
(D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner.

18 U.S.C. § 3553(a)(2).

B. The Court Should Impose Sentences within the Stipulated Guidelines Ranges

The Hacking Scheme was an extremely serious crime. It went on for years and resulted in hundreds of thousands of dollars of profit for the conspirators. It was highly technically sophisticated, and also involved the corruption of individual employees at JFK. It involved a

number of conspirators directly involved in the crime, as well as dozens or hundreds of taxi drivers. The conspiracy took place in both the United States and Russia, and the conspirators made extensive efforts to conceal their criminal activity.

Responding to the Hacking Scheme imposed huge costs on the Port Authority, which spent *years* attempting to address and defeat it. Individual taxi drivers were also, if not statutory victims of the scheme, certainly victims in a real sense. Every taxi driver who refused to pay, and had to wait longer for a fare as the conspirators repeatedly jumped paying taxi drivers to the front of the line, is a victim. So is every taxi driver who felt compelled to pay $10 per fare to avoid being pushed to the back of the line. Both Abayev and Leyman drove taxis themselves. As a result, they fully understood the harm their scheme caused to other taxi drivers, but they nonetheless carried on with the hacking out of greed.[3]

Abayev was the leader of the scheme. He conceived of it, he recruited the other participants, he directed it, and he controlled the distribution of the proceeds. Absent a statutory maximum, his sentencing Guidelines would be 87 to 108 months, and the Government would advocate for such a sentence if it was available. The statutory maximum, however, is approximately one third below the bottom of the Guidelines range. A sentence at the statutory maximum for Abayev is no greater than necessary to serve the purposes of sentencing.[4]

Leyman had a lesser role in the scheme, and he is substantially less culpable than Abayev. However, Leyman did engage in the conduct for a substantial length of time, and he did receive the same share of the proceeds that Abayev did. The sentencing Guidelines range of 57 to 60 months accurately captures his culpability, and such a sentence is sufficient but no greater than necessary to serve the purposes of sentencing.

V. Restitution and Forfeiture

The defendants are responsible for a total loss amount of $3,456,169.50, representing the total loss to the Port Authority from the Hacking Scheme. The defendants are jointly and severally liable for that amount in restitution, and the Government will submit restitution orders to the Court.

---

[3] Leyman's sentencing submission says that one of the reasons he engaged in the scheme was the financial distress caused by the COVID-19 pandemic. Leyman Memo at 4. However, Leyman began participating in the scheme in November 2019, several months before the pandemic.

[4] [redacted]

Each defendant made approximately $161,858.26 from the scheme, and each defendant has previously signed a preliminary forfeiture order in that amount. The Government respectfully requests that the forfeiture orders be made final.[5]

VI. Conclusion

For the reasons set forth above, the Government respectfully requests that the Court impose a sentence of 60 months' imprisonment as to Abayev and a sentence of between 57 to 60 months' imprisonment at to Leyman.

Respectfully submitted,

DAMIAN WILLIAMS
United States Attorney

by: /s/
Kevin Mead
Steven Kochevar
Assistant United States Attorneys
(212) 637-2211/2262

cc: All Counsel of Record (ECF)

[5] The preliminary forfeiture order for Abayev is at Dkt. 39. The preliminary forfeiture order for Leyman was transmitted to the Court by email on September 5, 2023, but does not appear to have been docketed.